Commissariat
à la protection de la
vie privée du Canada

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LES ENVIRONNEMENTS SANS FIL : EXAMEN DE CERTAINES INSTITUTIONS FÉDÉRALES

Rapport de vérification de la commissaire à la protection de la vie privée du Canada

Article 37 de la *Loi sur la protection des renseignements personnels*

RAPPORT FINAL

2010

Commissariat à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

613-947-1698, 1-800-282-1376
Téléc. : 613-947-6850
ATS : 613-992-9190
Suivez-nous sur Twitter : @privacyprivee

Nº de catalogue IP54-33/2010
ISBN 978-1-100-52313-2

Cette publication est également disponible sur notre site Web à **www.priv.gc.ca**.

Table des matières

Points principaux

ORGANISATIONS EXAMINÉES

Cinq organisations ont été sélectionnées pour la présente vérification : la Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada. Ces entités ont été choisies en raison de leur degré d'utilisation des technologies sans fil pour transmettre et conserver des renseignements personnels, du nombre de points d'accès à leurs réseaux sans fil, ainsi que du nombre d'employés qui disposent de dispositifs sans fil portatifs.

Nous avons passé en revue leurs politiques, procédures et pratiques de gestion des téléphones intelligents, des téléphones cellulaires et des réseaux sans fil (Wi-Fi). Nous avons voulu déterminer si les entités faisant l'objet de la vérification avaient évalué les menaces et les risques des technologies sans fil et adopté des mesures visant à minimiser ces risques. Nous avons examiné les contrôles en place pour protéger les renseignements personnels gérés dans un environnement sans fil, y compris l'utilisation de mots de passe, le cryptage et les restrictions sur l'utilisation de la messagerie NIP à NIP.

Nous avons également testé les dispositifs sans fil excédentaires (téléphones intelligents et cellulaires) et effectué un balayage afin de déceler les points d'accès sans fil dans les lieux occupés par les entités visées par la vérification ou dans les environs immédiats.

IMPORTANCE DE L'EXAMEN

Grâce à la technologie sans fil, les périphériques se servent des fréquences radio pour transmettre des données plutôt que des connexions câblées que l'on retrouve dans un environnement filaire contrôlé. La transmission sans fil des données constitue une méthode de télécommunication fondamentalement ouverte.

Dans le cadre de leur travail, des milliers de fonctionnaires fédéraux se sont vu attribuer des téléphones intelligents. La portabilité de ces dispositifs permet aux utilisateurs d'avoir accès à des renseignements confidentiels et d'en discuter lorsqu'ils font la file au guichet automatique, attendent l'embarquement dans un aéroport ou utilisent le transport en commun. Les dossiers qui se trouvent dans un ordinateur de bureau ou le réseau d'une organisation peuvent être transférés et conservés dans ces dispositifs. Par ricochet, ces dispositifs peuvent conserver de grandes quantités de renseignements personnels. L'utilisation inappropriée, le vol ou la perte de ces dispositifs peut exposer ces données au grand jour.

Les entités examinées offrent des services et des programmes dont dépendent les Canadiennes et les Canadiens. La prestation de ces services et programmes exige l'utilisation de renseignements personnels délicats, dont des renseignements fournis par les personnes qui cherchent à obtenir de l'aide auprès de l'un des programmes de logement gérés par la Société canadienne d'hypothèques et de logement; de l'information sur les personnes incarcérées pendant plus de deux ans; des données sur les soins de santé offerts aux résidents de quelque 200 communautés des Premières nations; des renseignements sur les prestataires du Régime de pensions du Canada, de la Sécurité de la vieillesse et de l'assurance-emploi; et de l'information sur les membres des Premières nations, les Inuits et les Métis.

Ces entités ont l'obligation de veiller à mettre en place des mesures techniques, physiques et administratives pour protéger l'intégrité et la sécurité des renseignements personnels qu'elles transmettent et conservent dans ces environnements sans fil.

CONSTATATIONS

La Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada ont adopté des politiques, procédures et processus de gestion des renseignements personnels transmis et conservés dans leurs environnements sans fil. Nous avons toutefois ciblé des faiblesses qui doivent être corrigées.

Même si diverses mesures de sécurité sont en place pour protéger les réseaux sans fil (Wi-Fi) et les dispositifs portatifs, aucune des entités examinées n'a vraiment évalué les menaces et les risques associés aux technologies sans fil. En l'absence de telles analyses, les entités soumises à la vérification sont incapables de démontrer que tous les risques inhérents au matériel ont été ciblés et convenablement gérés.

Les contrôles en matière de politiques et de procédures doivent être renforcés pour veiller à ce que les dispositifs sans fil ne deviennent pas la source d'une atteinte à la protection des données. Seulement trois des cinq entités soumises à la vérification ont adopté des protocoles de protection par mot de passe robuste pour les téléphones intelligents. Aucune des entités n'exige que les données conservées dans la mémoire de ces dispositifs soient chiffrées, et quatre des cinq entités ne disposent pas de procédures documentées visant à limiter le risque d'une atteinte à la protection des données en cas de perte ou de vol d'un dispositif.

La portabilité des dispositifs sans fil permet aux utilisateurs de mener des affaires dans les lieux publics, mais cela entraîne le risque que des renseignements personnels soient accidentellement exposés aux personnes qui les entourent. Des conseils et une formation appropriés permettent de minimiser ce risque. À une seule exception, nous avons constaté que les entités n'éduquent généralement pas les utilisateurs de sans-fil sur la manière d'utiliser les dispositifs de façon à protéger la vie privée.

Le Centre de la sécurité des télécommunications Canada (CSTC) est l'organisme national de cryptologie du Canada. Dans le cadre de son mandat, le CSTC offre des avis et des conseils aux ministères et organismes fédéraux pour les aider à sécuriser leurs systèmes et réseaux électroniques. Parmi les réseaux Wi-Fi examinés, nous avons déterminé que les niveaux de cryptage variaient parmi les quatre entités soumises à la vérification qui utilisaient cette technologie. Les niveaux de cryptage des réseaux Wi-Fi de trois entités correspondaient aux niveaux recommandés par le CSTC.

La messagerie NIP à NIP est une communication directe entre deux téléphones intelligents qui contourne le serveur de groupe d'une organisation. Compte tenu des vulnérabilités en matière de sécurité de ce type de communication, le CSTC a recommandé aux ministères de s'abstenir d'utiliser cette technologie et d'en désactiver la fonctionnalité sur les téléphones intelligents. Si un ministère a une exigence précise quant à la messagerie NIP à NIP (p. ex. l'intervention en cas d'urgence), le CSTC recommande qu'une politique claire sur son utilisation soit adoptée et que des mesures additionnelles soient mises en œuvre afin de protéger la vie privée et la confidentialité de ces communications.

Nous avons constaté que, contrairement à la recommandation du Centre de la sécurité des télécommunications Canada, toutes les entités soumises à la vérification autorisent la messagerie NIP à NIP. Par ailleurs, aucune entité n'a été en mesure de démontrer qu'elle avait adopté des mesures pour faire face aux enjeux de sécurité liés à l'utilisation de cette méthode de communication.

Finalement, nous avons noté des faiblesses dans la gestion des dispositifs sans fil excédentaires. Les ministères et organismes ont la responsabilité exclusive de la prévention de la communication non autorisée des renseignements contenus dans les biens excédentaires. Quatre des cinq entités n'ont pu démontrer que les données contenues dans tous les téléphones intelligents et cellulaires sont effacées (épurées) avant que les appareils ne soient liquidés.

Les réponses de la Société canadienne d'hypothèques et de logement, du Service correctionnel du Canada, de Santé Canada, de Ressources humaines et Développement des compétences Canada, et d'Affaires indiennes et du Nord Canada figurent à l'annexe du présent rapport.

Introduction

CONTEXTE

1. L'utilisation des télécommunications sans fil a augmenté considérablement. Les technologies sans fil incluent les réseaux Wi-Fi et les téléphones intelligents (comme le BlackBerry). La puissance de traitement et la connectivité de ces appareils permet aux utilisateurs d'accéder à des données en des lieux où il n'était pas possible de le faire auparavant.

2. Les capacités de traitement et d'entreposage des dispositifs sans fil en font des outils attrayants et précieux pour la prestation des services et l'exécution des programmes. Les appareils portatifs peuvent traiter les dossiers et les demandes que l'on retrouve habituellement dans les ordinateurs de bureau, et les données d'un réseau organisationnel peuvent être transférées à ces dispositifs assez facilement.

3. Qu'elles soient utilisées pour la transmission de données ou la communication vocale, les technologies sans fil offrent flexibilité et commodité aux fonctionnaires appelés à se déplacer. Ces technologies apportent de nombreux avantages, mais elles peuvent également mettre des renseignements personnels en danger.

4. Cinq organisations ont fait l'objet de la présente vérification : la Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada.

5. Ces entités offrent des programmes et des services qui exigent l'utilisation de renseignements personnels délicats. La Société canadienne d'hypothèques et de logement doit avoir accès à des renseignements pour pouvoir aider les Canadiennes et les Canadiens qui ont besoin d'un logement sûr et abordable. Le Service correctionnel du Canada conserve de l'information sur les personnes incarcérées pendant plus de deux ans. À titre de fournisseur de soins de santé primaires auprès de quelque 200 communautés des Premières nations, Santé Canada conserve les dossiers de soins de santé de milliers de personnes. Ressources humaines et Développement des compétences Canada gère les renseignements personnels des bénéficiaires de prestations du Régime de pensions du Canada, de la Sécurité de la vieillesse et de l'assurance-emploi. Affaires indiennes et du Nord Canada appuie les Premières nations, les Inuits et les Métis dans leurs efforts pour améliorer leur bien-être social et économique.

OBJET DE LA VÉRIFICATION

6. La vérification visait à déterminer si les entités choisies disposent de contrôles adéquats — y compris des politiques, procédures et processus — pour protéger les renseignements personnels transmis et conservés dans des environnements sans fil. Nous avons examiné les cadres de sécurité du réseautage sans fil et l'utilisation des dispositifs sans fil portatifs.

7. La vérification ne comportait pas d'examen des pratiques globales de traitement des renseignements personnels des entités ou de leurs infrastructures obligatoires de sécurité de la technologie de l'information. D'autres renseignements sur l'objectif, la portée, l'approche et les critères de la vérification figurent à la section **Au sujet de la vérification** du présent rapport.

Observations et recommandations

POLITIQUES ET PROCÉDURES DE CONTRÔLE

8. La Politique sur la sécurité du gouvernement du Conseil du Trésor et les normes connexes prévoient des mesures pour protéger et préserver la confidentialité et l'intégrité des fonds gouvernementaux, y compris des renseignements personnels. Ces instruments établissent les exigences de base (obligatoires) en matière de sécurité.

9. Les entités fédérales sont tenues de procéder à leurs propres évaluations pour déterminer si des mesures allant au-delà des exigences de base précisées dans la politique sont nécessaires. La politique exige également une surveillance constante des menaces pour veiller au maintien des mesures de sécurité appropriées.

10. Nous nous attendions à ce que la Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada aient :

    - évalué les menaces et les risques associés à leurs technologies sans fil (téléphones intelligents et réseaux Wi-Fi);
    - offert des conseils aux employés sur l'utilisation acceptable des téléphones intelligents et cellulaires;
    - défini un processus visant les dispositifs sans fil perdus ou volés;
    - mis en œuvre des exigences relatives à la sécurité, comme l'utilisation de mots de passe et le cryptage pour protéger les renseignements personnels dans les environnements sans fil;
    - veillé à ce que l'utilisation de la messagerie NIP à NIP respecte les consignes émises par le Centre de la sécurité des télécommunications Canada;
    - défini des procédures pour le retrait sécuritaire des téléphones intelligents et cellulaires excédentaires.

Les risques et les menaces n'ont pas été évalués de manière formelle

11. Si les technologies sans fil sont implantées en l'absence de mesures de sécurité adéquates, elles risquent d'offrir un accès absolu au réseau et aux données d'une organisation. Une évaluation des menaces et des risques (EMR) définit les menaces, évalue les risques connexes et recommande des mesures d'atténuation des vulnérabilités ciblées. L'évaluation permet également de valider si les normes minimales exigées dans la politique du Conseil du Trésor sont appropriées pour le genre d'informations transmises et conservées dans un environnement sans fil.

12. Même si divers niveaux de sécurité sont en place pour protéger les réseaux et les dispositifs sans fil, nous avons déterminé que la Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, et Affaires indiennes et du Nord Canada n'ont pas mené d'EMR de leurs réseaux sans fil. Nous avons constaté que le Service correctionnel du Canada a mené une évaluation de la vulnérabilité de son installation Wi-Fi. Même si la politique du Conseil du Trésor reconnaît que les deux types d'évaluation se chevauchent quelque peu, une évaluation de la vulnérabilité ne vise pas à cerner l'ensemble des menaces et des risques associés à une technologie ou un environnement donné. En l'absence de telles analyses, les

entités n'ont pu démontrer que les contrôles existants sur leurs réseaux sans fil et téléphones intelligents sont suffisants. Ressources humaines et Développement des compétences Canada terminait une EMR au moment de l'évaluation.

13. RECOMMANDATION

La Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, et Affaires indiennes et du Nord Canada devraient évaluer les risques pour la sécurité et la protection des renseignements personnels associés aux réseaux sans fil et aux téléphones intelligents en se livrant à une évaluation des menaces et des risques.

Des conseils limités sont offerts sur la façon de protéger les renseignements personnels dans le cadre de l'utilisation des téléphones intelligents

14. La portabilité des dispositifs sans fil permet aux utilisateurs de mener des affaires durant leurs déplacements. Des discussions qui traditionnellement se déroulaient derrière des portes closes peuvent maintenant avoir lieu dans des endroits publics. Il y a donc risque que des renseignements personnels soient accidentellement exposés aux personnes qui les entourent.

15. Nous nous attendions à constater que les entités évaluées avaient offert des conseils à leurs employés afin de veiller à ce que les dispositifs sans fil soient utilisés d'une manière qui respecte la vie privée. Nous avons évalué les entités afin de déterminer si elles sensibilisent les employés aux risques associés à l'utilisation des téléphones intelligents. Puis, nous avons vérifié les réponses reçues dans le cadre des entrevues. Nous avons également examiné les ententes que doivent signer les utilisateurs lorsqu'ils reçoivent un téléphone intelligent.

16. À une seule exception, aucune des entités n'a pu démontrer que les utilisateurs de téléphones intelligents avaient reçu une formation précise sur la protection des renseignements personnels pour traiter d'enjeux comme les mesures de protection des données emmagasinées dans les dispositifs sans fil et les répercussions de l'utilisation de la technologie dans les lieux publics.

17. La Société canadienne d'hypothèques et de logement a mis en œuvre diverses initiatives de formation, y compris des présentations et des guides d'orientation sur la sécurité à l'intention de divers publics internes. Celles-ci traitent de façon approfondie des responsabilités des utilisateurs d'un sans-fil, des types de renseignements qui peuvent être transmis, des solutions qui permettent de protéger les dispositifs et des enjeux liés à la sécurité du sans-fil.

18. Nous avons également constaté que Ressources humaines et Développement des compétences Canada a mené une campagne de conscientisation pour rappeler aux employés que des discussions où l'on aborde des renseignements personnels ne devraient pas se dérouler dans des lieux publics où il existe un risque élevé d'être entendu.

19. L'entente qu'une organisation demande à l'utilisateur d'un sans-fil de signer traite des questions d'administration et de sécurité liées au fonctionnement du téléphone intelligent ou cellulaire. Aucune des ententes ne contenait de dispositions sur la responsabilité des utilisateurs quant au respect de la vie privée.

20. RECOMMANDATION

Le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada devraient veiller à ce que les employés soient conscients des risques d'entrave à la vie privée inhérents à l'utilisation de téléphones intelligents et offrir des conseils pour limiter ces risques.

Les processus relatifs à la perte et au vol de téléphones intelligents n'ont pas été officialisés

21. Réagir rapidement au vol ou à la perte d'un dispositif sans fil minimisera le risque que des renseignements personnels soient compromis. Nous nous attendions à ce que les entités soumises à la vérification disposent de procédures documentées pour faire face à de telles éventualités.

22. Nous avons constaté que les pratiques variaient d'une entité à l'autre et, dans certains cas, au sein même de l'entité vérifiée. Même si les utilisateurs sont tenus de signaler la perte ou le vol d'un téléphone intelligent, une seule entité — la Société canadienne d'hypothèques et de logement (SCHL) — a été en mesure de fournir les procédures documentées décrivant les étapes à suivre pour limiter le risque d'une atteinte à la protection des données. Le processus prévoit l'effacement des données, la désactivation du dispositif sans fil et le retrait de l'utilisateur du serveur. Le groupe responsable de la gestion des risques et de la sécurité à la SCHL mène une enquête sur chaque téléphone intelligent perdu ou volé, confirme que les données ont été effacées et que le dispositif a été désactivé, et prépare un rapport de résultats mensuel à l'intention du président de la SCHL. Nous avons toutefois noté que la Société était incapable de démontrer que ce processus est suivi sur une base régulière. La SCHL a indiqué qu'elle passerait en revue ses procédures et outils pour veiller à ce que les risques résiduels, le cas échéant, soient adéquatement atténués.

23. En l'absence de procédures documentées et de l'assurance qu'elles sont uniformément appliquées, les renseignements personnels risquent d'être exposés. Par exemple, nous avons été informés qu'à certaines occasions, un fournisseur de services de télécommunications a été informé de la perte ou du vol d'un dispositif sans fil avant qu'une commande de nettoyage n'ait été envoyée. Une fois qu'un téléphone intelligent est mis hors service, sa capacité à transmettre ou à recevoir un message est désactivée. Par conséquent, le dispositif ne peut être nettoyé et les données qui s'y trouvent — y compris les renseignements personnels — y resteront emmagasinées.

24. RECOMMANDATION

Le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada devraient adopter des procédures documentées pour réagir à la perte ou au vol de dispositifs sans fil.

MESURES DE SÉCURITÉ VISANT LES RENSEIGNEMENTS PERSONNELS

Le manque de mots de passe robustes et l'absence de cryptage dans les téléphones intelligents menacent la protection de la vie privée

25. Les téléphones intelligents sont largement répandus au sein du gouvernement fédéral. Ils sont configurés pour fonctionner avec un compte de courriel d'entreprise et ont la capacité d'emmagasiner des milliers de courriels et de pièces jointes. Pour protéger le droit à la vie privée et réduire le risque d'une communication non autorisée de renseignements personnels, nous nous attendions à ce que les entités soumises à la vérification aient adopté des politiques claires et des exigences de sécurité de base pour les dispositifs sans fil.

26. L'utilisation de mots de passe et le cryptage sont des mesures de sécurité importantes qui permettent de protéger les renseignements personnels emmagasinés dans les téléphones intelligents et transmis par ces derniers. Ces mesures permettent d'assurer que seules les personnes autorisées à accéder aux données peuvent le faire. Nous avons examiné la façon dont les entités soumises à la vérification configuraient leurs serveurs

d'entreprise pour les téléphones intelligents. Nous avons également interrogé le personnel affecté à la technologie de l'information et les gestionnaires responsables de la sécurité.

27. Le Centre de la sécurité des télécommunications Canada recommande l'utilisation de mots de passe robustes pour toutes les affaires gouvernementales. Un mot de passe robuste doit comporter au moins huit caractères, dont des lettres majuscules et minuscules, des nombres et des symboles.

28. Nous avons constaté que Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada ont adopté des protocoles de protection par mot de passe robuste pour les téléphones intelligents. Le Service correctionnel du Canada exige l'utilisation d'un mot de passe pour protéger ses téléphones intelligents, mais ne précise pas qu'il doit contenir les éléments d'un mot de passe robuste. Même si la Société canadienne d'hypothèques et de logement encourage fortement l'utilisation de mots de passe dans diverses politiques et communications, la décision d'activer la caractéristique du mot de passe revient à l'utilisateur du sans-fil.

29. Le cryptage est un processus de transformation qui rend l'information illisible, sauf pour les personnes qui détiennent ce qu'on appelle une « clé ». Le cryptage est généralement utilisé pour protéger l'information contenue dans divers types de systèmes. Aucune des entités soumises à la vérification n'exige que les données soient cryptées dans la mémoire des dispositifs sans fil. Le cryptage des données ajoute un niveau de sécurité, ce qui permet de réduire le risque associé à l'accès non autorisé aux données dans l'éventualité où un dispositif est perdu ou volé.

30. L'absence de mots de passe robustes et de cryptage présente un risque important pour la vie privée. Les conséquences peuvent être graves, les téléphones intelligents pouvant conserver d'importantes quantités de renseignements personnels.

31. RECOMMANDATION

La Société canadienne d'hypothèques et de logement et le Service correctionnel du Canada devraient exiger l'utilisation de mots de passe robustes pour leurs téléphones intelligents.

32. RECOMMANDATION

La Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada devraient veiller à ce que les données conservées dans les téléphones intelligents soient cryptées.

Les messages NIP à NIP peuvent être interceptés

33. La messagerie NIP à NIP — également connue sous le nom de messagerie de « poste à poste » — est une communication directe entre les téléphones intelligents sur le réseau BlackBerry. Les messages sont adressés à un « NIP » (unique à chaque téléphone intelligent) plutôt qu'à une adresse de courriel. Les messages sont acheminés directement par le réseau hôte de transmission des télécommunications, contournant ainsi les serveurs d'une organisation.

34. Les messages NIP à NIP peuvent facilement être interceptés à l'aide de matériel à la fois bon marché et facilement accessible. Les bulletins de sécurité des TI émis par le Centre de la sécurité des télécommunications Canada (CSTC) en octobre 2008 et janvier 2010 mettent en lumière la nature non sécuritaire de cette méthode de communication. Par ailleurs, les bulletins soulignent que la messagerie NIP à NIP n'est pas adaptée

à l'échange de renseignements délicats et recommandent que les ministères et organismes s'abstiennent d'utiliser cette technologie. Si une institution a une exigence particulière pour la messagerie NIP à NIP (p. ex. pour les services d'urgence), le CSTC recommande d'appliquer une politique claire sur son utilisation et d'adopter des mesures additionnelles pour assurer le respect de la vie privée et la confidentialité de ces communications. Nous avons examiné la configuration des téléphones intelligents pour déterminer si les entités faisant l'objet de la vérification suivent les directives du CSTC.

35. Nous avons constaté que, contrairement à la recommandation du CSTC, toutes les entités soumises à la vérification autorisaient la messagerie NIP à NIP. Par ailleurs, aucune des entités n'a pu démontrer qu'elle avait adopté des mesures pour traiter des enjeux de sécurité afférents à l'utilisation de cette méthode de communication.

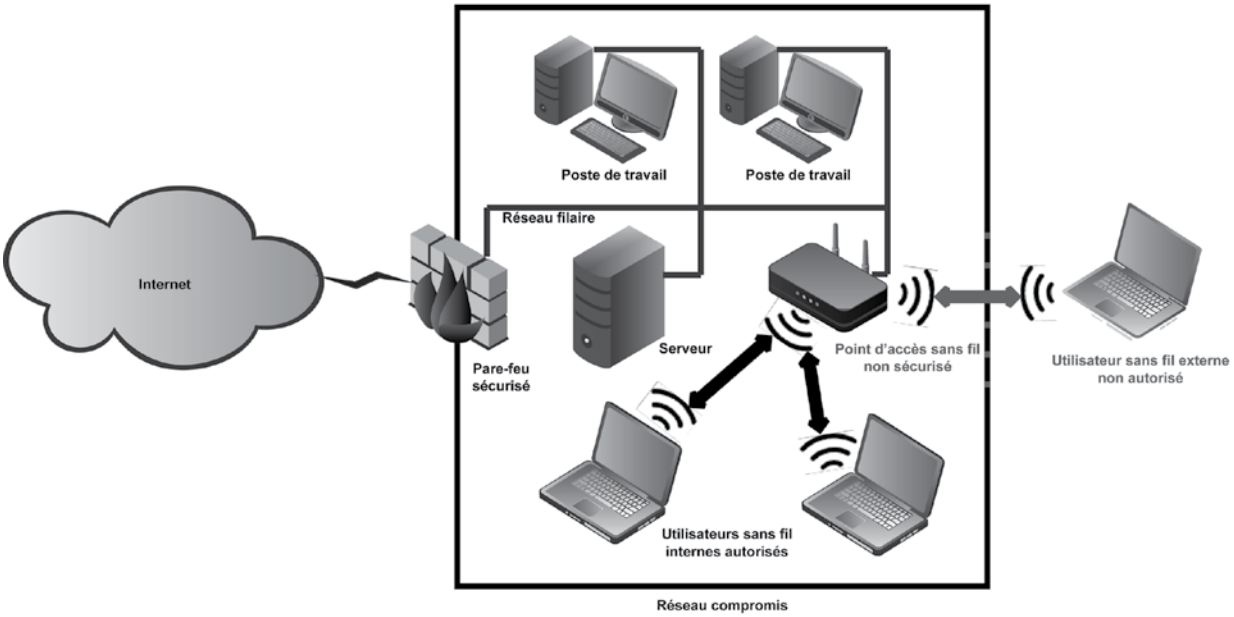
36. RECOMMANDATION

La Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada devraient veiller à ce que l'utilisation de la messagerie NIP à NIP soit conforme aux directives émises par le Centre de la sécurité des télécommunications Canada.

Les points d'accès sans fil offrent des degrés de protection variables

37. L'informatique sans fil (Wi-Fi) est de plus en plus utilisée par les entreprises, les gouvernements et les particuliers. Les réseaux Wi-Fi se servent des ondes radioélectriques pour transmettre des

Un point d'accès dans un réseau sans fil indésirable ou non protégé permet l'accès externe non autorisé à un réseau d'entreprise en contournant la sécurité offerte par le pare-feu.



Source : Compilation effectuée par le Commissariat à la protection de la vie privée du Canada

données à des dispositifs dotés d'une connectivité sans fil (p. ex. des ordinateurs portatifs).

38. Les réseaux sans fil peuvent être exploités par des personnes qui, à l'aide d'ordinateurs portatifs spécialement équipés, peuvent détecter les signaux provenant de transmissions sans fil, ce qui permet à l'intrus potentiel de cibler les points d'accès dont le cryptage est faible ou non sécurisé. Une fois cette vulnérabilité détectée, diverses attaques peuvent être lancées. Ces attaques peuvent comprendre la saisie, la modification ou la suppression de messages, ou l'utilisation des privilèges d'un utilisateur autorisé pour accéder à un système. Par conséquent, nous nous attendions à ce que les réseaux Wi-Fi des entités soient protégés par un système de cryptage de sécurité robuste.

39. Dans le cadre de nos examens, nous avons contrôlé l'espace occupé par les installations des entités soumises à la vérification et l'espace attenant. Cette activité de surveillance est connue sous l'appellation « piratage Wi-Fi ». Nous avons examiné les détails de transport des transmissions pour déterminer leur origine et le niveau de cryptage, mais nous n'avons pas examiné le contenu des communications.

40. Nous n'avons pu détecter aucune installation Wi-Fi à Ressources humaines et Développement des compétences Canada.

41. Les niveaux de cryptage utilisés pour limiter la menace d'exposition des données variaient parmi les quatre autres entités soumises à la vérification. Nous avons constaté que les niveaux de cryptage des réseaux Wi-Fi de la Société canadienne d'hypothèques et de logement et d'Affaires indiennes et du Nord Canada correspondent à ceux recommandés par le Centre de la sécurité des télécommunications Canada. Le Service correctionnel du Canada utilise de façon limitée la technologie Wi-Fi. À la lumière de notre examen de sa configuration, nous sommes convaincus que les mesures appropriées sont en place pour protéger les transmissions de données sur le réseau.

42. Santé Canada utilise l'informatique Wi-Fi dans certains endroits éloignés. Même si nous n'avons pas vérifié les niveaux de cryptage à ces endroits, des fonctionnaires du Ministère nous ont indiqué que le cryptage de sécurité utilisé ne respecte pas le niveau recommandé par le Centre de la sécurité des télécommunications Canada.

43. RECOMMANDATION

Santé Canada devrait passer en revue ses réseaux sans fil et s'assurer que les points d'accès sont dotés du cryptage de sécurité recommandé par le Centre de la sécurité des télécommunications Canada.

PRATIQUES DE RETRAIT

En général, les entités entreposent les dispositifs sans fil excédentaires de façon sécuritaire

44. Les entités fédérales sont tenues de veiller à ce que les renseignements personnels en attente de retrait soient conservés de façon sécuritaire. Elles doivent également veiller à ce que l'on procède au retrait de l'information d'une manière qui ne compromet pas le droit à la vie privée.

45. Nous avons examiné les processus que doivent suivre les employés lorsqu'ils veulent se départir de dispositifs sans fil et effectué des visites dans les installations des entités soumises à la vérification où l'on recueille et entrepose des téléphones intelligents et cellulaires, tant à l'administration centrale que dans les bureaux régionaux. Nous avons également interviewé les gestionnaires et les employés responsables de veiller à ce que les données soient effacées des dispositifs.

46. Dans l'ensemble, les entités soumises à la vérification entreposent des milliers de dispositifs sans fil excédentaires. Les méthodes d'entreposage des dispositifs varient. À l'exception de Ressources humaines et Développement des compétences

Canada (RHDCC), toutes les entités ont mis en œuvre des mesures sécurisées visant à protéger ces biens. Nous avons constaté que les dispositifs sans fil excédentaires sont entreposés dans des classeurs verrouillés ou des salles sécuritaires, où l'accès est limité.

47. Dans un bureau régional de RHDCC, nous avons toutefois constaté que les téléphones intelligents et cellulaires excédentaires étaient entreposés dans un classeur non verrouillé, accessible à l'ensemble du personnel. Nous avons contrôlé un échantillon des dispositifs conservés à cet endroit et découvert que certains contenaient des données.

48. RECOMMANDATION

Ressources humaines et Développement des compétences Canada devrait veiller à ce que tous ses dispositifs sans fil excédentaires soient entreposés dans des zones sécurisées.

Les données ne sont pas effacées de tous les téléphones intelligents et cellulaires

49. Les ministères et organismes fédéraux se départissent habituellement de leurs biens excédentaires par l'intermédiaire de la Distribution des biens de la Couronne de Travaux publics et Services gouvernementaux Canada, l'organisation responsable de la vente, de la distribution, du retrait et de la réutilisation des biens fédéraux excédentaires.

50. Les dispositifs sans fil excédentaires peuvent représenter un important risque pour la vie privée si les données qu'ils contiennent ne sont pas nettoyées (épurées) avant qu'ils ne soient liquidés, sans égard à la méthode de retrait utilisée (p. ex. la destruction physique ou le transfert à Distribution des biens de la Couronne pour être offerts aux enchères publiques). Le ministère ou l'organisme d'origine (ou chargé de l'aliénation) a la responsabilité de veiller à ce que cela soit fait.

51. Nous avons contrôlé un échantillon de dispositifs sans fil excédentaires de toutes les entités soumises à la vérification, à l'exception de la Société canadienne d'hypothèques et de logement. Nous avons demandé à la Société de nous fournir les documents (p. ex. les feuilles de contrôle, les journaux) permettant de démontrer que les dispositifs excédentaires ont été épurés. Même si la Société dispose d'un processus pour épurer les données des téléphones excédentaires, elle ne maintient pas de listes de contrôle lui permettant de vérifier que toutes les étapes du processus ont été, dans tous les cas, suivies.

52. Nous avons constaté que les données de tous les téléphones intelligents et cellulaires excédentaires d'Affaires indiennes et du Nord Canada ont été épurées. Il n'en était pas de même au Service correctionnel du Canada, à Santé Canada, et à Ressources humaines et Développement des compétences Canada, où nous avons trouvé des données dans plusieurs dispositifs excédentaires destinés au retrait.

53. RECOMMANDATION

La Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, et Ressources humaines et Développement des compétences Canada devraient établir des mécanismes de contrôle pour s'assurer que les données conservées dans les dispositifs sans fil excédentaires sont effacées avant la liquidation de ces dispositifs.

Conclusion

54. Même si diverses mesures de sécurité sont en place pour protéger les réseaux sans fil (Wi-Fi) et les dispositifs portatifs, aucune des entités soumises à la vérification n'a pleinement évalué les menaces et les risques afférents à l'utilisation des technologies sans fil. En l'absence de telles analyses, il n'y a aucun moyen de confirmer que tous les risques importants ont été ciblés et réduits de manière appropriée.

55. Parmi les réseaux Wi-Fi examinés, nous avons constaté que les niveaux de cryptage variaient entre les quatre entités qui ont adopté la technologie. Trois des quatre entités ont mis en place le cryptage de sécurité qui répond au niveau recommandé par le Centre de la sécurité des télécommunications Canada. L'autre ministère utilise une forme de cryptage moins perfectionnée.

56. Des mesures de sécurité supplémentaires doivent être adoptées pour veiller à ce que les téléphones intelligents ne deviennent pas la source d'une atteinte à la protection des données. Seulement trois des cinq entités ont adopté une exigence de protection par mot de passe robuste pour leurs téléphones intelligents, et aucune n'exige que les données conservées dans la mémoire de ces dispositifs soient cryptées.

57. On note des lacunes importantes dans les politiques actuelles qui entourent les dispositifs sans fil — y compris en ce qui concerne les restrictions sur l'utilisation de la messagerie NIP à NIP — et quatre des cinq entités ne disposent pas de procédures documentées visant à limiter le risque d'une atteinte à la protection des données en cas de perte ou de vol d'un dispositif sans fil. Par ailleurs, à une exception près, les entités ne sensibilisent généralement pas les utilisateurs aux risques d'entrave à la vie privée associés aux dispositifs sans fil, ou à l'utilisation de ces derniers dans le respect du droit à la vie privée.

58. Finalement, les contrôles existants pour gérer les dispositifs sans fil excédentaires ne sont pas adéquats. Seulement une entité a réussi à démontrer que les mesures existantes donnaient l'assurance que les données sont épurées des téléphones intelligents et cellulaires avant qu'ils ne soient liquidés.

59. L'utilisation de technologies et de dispositifs sans fil pour transmettre et stocker des données entraîne certains risques pour la vie privée. En nous appuyant sur notre travail de vérification, nous avons conclu que la Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada doivent renforcer certaines politiques, procédures ou contrôles afin d'atténuer davantage ces risques.

Au sujet de la vérification

AUTORITÉ

L'article 37 de la *Loi sur la protection des renseignements personnels* confère à la commissaire à la protection de la vie privée l'autorité d'examiner la conformité des institutions fédérales en ce qui concerne la gestion de leurs fonds de renseignements personnels en plus de formuler les recommandations qu'elle juge appropriées.

OBJECTIF

La vérification visait à déterminer si la Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada disposent de contrôles adéquats — y compris des politiques, procédures et processus — pour protéger les renseignements personnels transmis et conservés dans des environnements sans fil.

CRITÈRES

Les critères utilisés pour mener cette vérification sont tirés de la *Loi sur la protection des renseignements personnels*, des politiques pertinentes du Conseil du Trésor, des principes généralement admis sur la protection de la vie privée, du IT Governance Institute, du cadre Control Objectives for Information and related Technology (COBIT® 4.1) et du cadre de la Bibliothèque d'infrastructure des technologies de l'information (BITI).

Nous nous attendions à ce que les organisations gouvernementales choisies aient :

- évalué les menaces et les risques associés aux technologies sans fil;
- offert des conseils aux employés sur l'utilisation acceptable des téléphones intelligents et cellulaires;
- défini un processus officialisé visant à répondre aux incidents de perte ou de vol de dispositifs sans fil;
- mis en œuvre des exigences de base relatives à la sécurité, comme l'utilisation de mots de passe robustes et du cryptage, pour protéger les renseignements personnels dans un environnement sans fil;
- veillé à ce que l'utilisation de la messagerie NIP à NIP respecte les consignes émises par le Centre de la sécurité des télécommunications Canada;
- défini des procédures pour le retrait sécuritaire des dispositifs sans fil excédentaires.

PORTÉE ET DÉMARCHE

Dans le cadre de la vérification, nous avons d'abord effectué une étude préparatoire auprès de 34 organisations gouvernementales pour obtenir un aperçu de l'utilisation du sans fil au gouvernement fédéral. Les cinq organisations soumises à la vérification doivent gérer des quantités importantes de renseignements personnels pour s'acquitter du mandat qui leur est conféré par la loi.

Nous avons interviewé le personnel et passé en revue les politiques, procédures et lignes directrices. Nous avons également examiné un échantillon de dispositifs sans fil excédentaires pour déterminer si toutes les données qu'ils contenaient avaient été effacées (épurées) avant que les dispositifs soient liquidés.

Finalement, nous avons contrôlé l'espace occupé par les installations des entités soumises à la vérification et l'espace attenant. Nous avons obtenu un avis juridique pour confirmer que notre activité à cet égard ne contrevenait pas aux lois provinciales ou fédérales.

Les activités de vérification ont été réalisées dans la région de la capitale nationale et à Toronto, Montréal, Québec, Winnipeg, Vancouver et Abbotsford.

Nos travaux de vérification étaient pour l'essentiel terminés le 30 août 2009.

NORMES DE VÉRIFICATION

La vérification a été effectuée en conformité avec les pratiques, les politiques et le mandat législatif du Commissariat à la protection de la vie privée du Canada, et conformément à l'esprit des normes de vérification recommandées par l'Institut canadien des comptables agréés.

ÉQUIPE DE LA VÉRIFICATION

Directeur général : Steven Morgan

Michael Fagan
Bill Wilson
Paul Zind

Annexe — Recommandations et réponses

Les risques et les menaces n'ont pas été évalués de manière formelle

RECOMMANDATION

La Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, et Affaires indiennes et du Nord Canada devraient évaluer les risques pour la sécurité et la protection des renseignements personnels associés aux réseaux sans fil et aux téléphones intelligents en se livrant à une évaluation des menaces et des risques.

Réponse de la Société canadienne d'hypothèques et de logement : La SCHL analyse les risques pour la sécurité et les stratégies de réduction des risques durant la mise en œuvre de toute fonctionnalité ou technologie sans fil. Les menaces et les risques sont passés en revue de manière continue et des améliorations sont adoptées au besoin. Les politiques sur la sécurité des TI et les politiques en matière de sécurité de l'information incluent également les politiques et les lignes directrices sur la façon de protéger les renseignements. Ces politiques sont communiquées à tous les employés par le biais de séances de formation, de communiqués et de bases de données en ligne. La SCHL n'a jamais eu de problèmes à cet égard.

Réponse du Service correctionnel du Canada : Le Service correctionnel du Canada (SCC) n'est pas entièrement d'accord avec la conclusion selon laquelle il n'aurait pas effectué d'évaluations des menaces et des risques de ses installations sans fil. Le SCC considère le volet Wi-Fi comme un prolongement de son réseau actuel. Une évaluation des menaces et des risques de son réseau sera mise à jour pour y inclure le volet Wi-Fi compte tenu des éléments de preuve recueillis dans les évaluations de la vulnérabilité et les examens de l'utilisation du sans-fil au sein de l'organisme.

Le SCC élabore actuellement un plan d'action pour prendre en compte le volet de la recommandation portant sur les téléphones intelligents.

Réponse de Santé Canada : Santé Canada convient qu'une évaluation des menaces et des risques (EMR) devrait être effectuée et indique qu'elle procédera à une EMR des réseaux sans fil et des téléphones intelligents.

Réponse d'Affaires indiennes et du Nord Canada : Affaires indiennes et du Nord Canada préparera une évaluation des menaces et des risques de ses réseaux et dispositifs sans fil ainsi que de ses téléphones intelligents afin de déterminer les risques pour la sécurité et la protection de la vie privée associés à ces systèmes, y compris le survol des évaluations des menaces et des risques existants de technologies précises, ainsi que d'autres évaluations des menaces et des risques de technologies précises, au besoin. Les risques ciblés et la stratégie d'atténuation seront présentés à la haute direction.

Des conseils limités sont offerts sur la façon de protéger les renseignements personnels dans le cadre de l'utilisation des téléphones intelligents

RECOMMANDATION

Le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada devraient veiller à ce que les employés soient conscients des risques d'entrave à la vie privée inhérents à l'utilisation de téléphones intelligents et offrir des conseils pour limiter ces risques.

Réponse du Service correctionnel du Canada : Le Service correctionnel du Canada est d'accord avec la recommandation et prépare actuellement un plan d'action pour remédier à la situation.

Réponse de Santé Canada : Santé Canada convient que les employés devraient être informés des risques d'entrave à la vie privée inhérents à l'utilisation des téléphones intelligents et fournira les conseils nécessaires pour atténuer ces risques. Santé Canada élargit la politique et l'entente relatives à l'utilisation des dispositifs sans fil pour inclure la responsabilité de l'utilisateur à se servir du dispositif en protégeant la confidentialité des renseignements personnels et des renseignements ministériels. Par ailleurs, la politique sur les dispositifs sans fil indiquera aux utilisateurs qu'ils doivent limiter l'utilisation des transmissions de nature non délicate et cette restriction comprendra la protection des renseignements personnels. Les utilisateurs seront avisés qu'ils ne devraient pas utiliser leurs dispositifs sans fil pour communiquer de l'information désignée sur les employés ou d'autres personnes.

Réponse de Ressources humaines et Développement des compétences Canada : Ressources humaines et Développement des compétences Canada accepte cette recommandation. Le Ministère mettra à jour son programme de sensibilisation à la sécurité des TI. En outre, le Ministère s'assurera que les employés sont mis au courant des risques pour la vie privée en présence lorsqu'ils utilisent des téléphones intelligents, et qu'ils reçoivent des directives pour atténuer ces risques.

Réponse d'Affaires indiennes et du Nord Canada : Il est reconnu qu'Affaires indiennes et du Nord Canada (AINC) doit élaborer ou mettre à jour des politiques, normes et lignes directrices concernant l'utilisation des dispositifs sans fil et intégrer les préoccupations liées à la protection de la vie privée dans ces documents. La Division de la sécurité des TI participe actuellement aux séances d'orientation des nouveaux employés et accroît la conscientisation sur la sécurité des TI auprès de tous les employés par le biais de séances de conscientisation, d'affiches, du bulletin électronique Express d'AINC et des mises à jour du site Web. L'unité responsable de la sécurité du Ministère et celle responsable de la protection de la vie privée améliorent également la conscientisation par le biais de divers moyens de communication. Le matériel devra être mis à jour pour mettre davantage l'accent sur les questions de protection de la vie privée liées à toutes les formes de télécommunication sans fil.

Les processus relatifs à la perte et au vol de téléphones intelligents n'ont pas été officialisés

RECOMMANDATION

Le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada devraient adopter des procédures documentées pour réagir à la perte ou au vol de dispositifs sans fil.

Réponse du Service correctionnel du Canada : Le Service correctionnel du Canada est d'accord avec la recommandation et prépare actuellement un plan d'action pour remédier à la situation.

Réponse de Santé Canada : Santé Canada convient que les employés devraient être informés des risques d'entrave à la vie privée inhérents à l'utilisation des téléphones intelligents et fournira les conseils nécessaires pour atténuer ces risques. Tous les nouveaux utilisateurs devront lire et signer l'entente à jour sur l'utilisation des dispositifs sans fil la première fois qu'ils se verront attribuer un dispositif sans fil. Cette entente s'appliquera également aux utilisateurs actuels de dispositifs sans fil. Elle inclura également les procédures pour répondre aux incidents de perte ou de vol de dispositifs sans fil..

Réponse de Ressources humaines et Développement des compétences Canada : Ressources humaines et Développement des compétences Canada accepte cette recommandation. Le Ministère dispose déjà de procédures nationales documentées pour l'utilisation de BlackBerrys et mettra en place un processus similaire pour les téléphones cellulaires, afin d'assurer l'uniformité à l'échelon national.

Réponse d'Affaires indiennes et du Nord Canada : Affaires indiennes et du Nord Canada dispose actuellement d'un processus documenté pour répondre aux incidents; le processus doit toutefois être mis à jour pour inclure les questions de protection de la vie privée relatives aux dispositifs sans fil perdus ou volés. Le processus à suivre en cas d'incident destiné aux employés doit être communiqué régulièrement. Par ailleurs, l'exigence de signaler les dispositifs perdus ou volés sera intégrée à la politique sur les dispositifs sans fil.

Le manque de mots de passe robustes et l'absence de cryptage dans les téléphones intelligents menacent la protection de la vie privée

RECOMMANDATION

La Société canadienne d'hypothèques et de logement et le Service correctionnel du Canada devraient exiger l'utilisation de mots de passe robustes pour leurs téléphones intelligents.

Réponse de la Société canadienne d'hypothèques et de logement : La SCHL a toujours recommandé fortement à ses employés d'utiliser la protection par mot de passe pour les téléphones intelligents dans ses diverses politiques et communications internes. Le 26 mai 2010, la protection obligatoire par mot de passe pour les BlackBerry et le cryptage des données ont été mis en place à la SCHL.

Réponse du Service correctionnel du Canada : Le Service correctionnel du Canada est d'accord avec la recommandation et prépare actuellement un plan d'action pour remédier à la situation.

RECOMMANDATION

La Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada devraient veiller à ce que les données conservées dans les téléphones intelligents soient cryptées.

Réponse de la Société canadienne d'hypothèques et de logement : La SCHL a toujours recommandé fortement à ses employés d'utiliser la protection par mot de passe pour les téléphones intelligents dans ses diverses politiques et communications internes. Le 26 mai 2010, la protection obligatoire par mot de passe pour les BlackBerry et le cryptage des données ont été mis en place à la SCHL.

Réponse du Service correctionnel du Canada : Le Service correctionnel du Canada est d'accord avec la recommandation et prépare actuellement un plan d'action pour remédier à la situation.

Réponse de Santé Canada : Santé Canada convient que les données conservées dans les téléphones intelligents devraient être cryptées. Santé Canada collabore actuellement avec des vendeurs de dispositifs sans fil pour élaborer des procédures et processus pour veiller à ce que les données aient été cryptées conformément aux normes du Centre de sécurité des télécommunications Canada (CSTC). Santé Canada déterminera la faisabilité d'inclure un chiffrement et une protection des données additionnelles pour le serveur d'entreprise BlackBerry (communément appelé BES), permettant ainsi aux utilisateurs de Santé Canada de respecter les exigences en matière de protection des données de la Politique sur la sécurité du gouvernement ainsi que les exigences du CSTC.

Réponse de Ressources humaines et Développement des compétences Canada : Ressources humaines et Développement des compétences Canada (RHDCC) accepte cette recommandation. Le Ministère reconnaît que la sécurité des données stockées sur des téléphones intelligents est assujettie à un certain niveau de risque. Le Ministère est prêt à participer à des discussions à l'échelon du gouvernement du Canada à ce sujet, afin de mieux comprendre les risques associés au stockage de données sur ces appareils et faciliter son évaluation des répercussions afin de prendre des décisions éclairées.

Réponse d'Affaires indiennes et du Nord Canada : Une évaluation des risques associés à la technologie sans fil actuellement utilisée par le Ministère sera effectuée. Les résultats des évaluations des risques, conjointement avec les recommandations fondées sur les directives du CSTC, seront le moteur de la mise en œuvre du cryptage requis dans le but de mieux protéger les renseignements délicats au sein d'Affaires indiennes et du Nord Canada.

Les messages NIP à NIP peuvent être interceptés

RECOMMANDATION

La Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, Ressources humaines et Développement des compétences Canada, et Affaires indiennes et du Nord Canada devraient veiller à ce que l'utilisation de la messagerie NIP à NIP soit conforme aux directives émises par le Centre de la sécurité des télécommunications Canada.

Réponse de la Société canadienne d'hypothèques et de logement : Les politiques de la SCHL indiquent clairement que la messagerie NIP à NIP doit être utilisée à l'occasion seulement, pour les situations urgentes, conformément aux plans de reprise des activités.

La SCHL a mis en place un processus dans le cadre duquel les nouveaux utilisateurs d'un BlackBerry doivent indiquer officiellement avoir lu toutes les politiques connexes et les conditions d'utilisation du dispositif, y compris celles concernant le recours à la messagerie NIP à NIP.

Réponse du Service correctionnel du Canada : Le Service correctionnel du Canada est d'accord avec la recommandation et prépare actuellement un plan d'action pour remédier à la situation.

Réponse de Santé Canada : Santé Canada convient que la messagerie NIP à NIP est incompatible avec les conseils émis par le CSTC. Dans le cas des utilisateurs qui ont des exigences précises en matière de messagerie NIP à NIP (p. ex. les communications d'urgence), la politique sur les dispositifs sans fil sera élargie pour inclure l'utilisation de la messagerie NIP à NIP et des mesures additionnelles seront utilisées pour protéger la vie privée et la confidentialité de la messagerie NIP à NIP. L'administrateur du serveur d'entreprise BlackBerry (BES) a l'option d'établir une clé de chiffrement NIP à NIP propre à l'organisation dans le BES. Il faut noter que cela a pour effet de remplacer la clé de chiffrement générale par défaut et limite la capacité de déchiffrer des messages NIP à NIP aux dispositifs BlackBerry du Ministère qui sont connectés au BES. Toutefois, cela contribue également à empêcher les communications NIP à NIP avec les dispositifs BlackBerry se trouvant à l'extérieur du Ministère, et pourrait empêcher les communications d'urgence avec les organisations externes. L'utilisation de cette fonction sera donc soigneusement pensée pour l'administrateur du BES qui utilise l'option d'établir une clé de chiffrement NIP à NIP propre à l'organisation.

Réponse de Ressources humaines et Développement des compétences Canada : Ressources humaines et Développement des compétences Canada accepte cette recommandation. Le Ministère reconnaît qu'une exigence opérationnelle clairement définie des communications NIP à NIP est indispensable à ses services d'infrastructure et prendra part à une approche concertée à l'échelon du gouvernement du Canada, qui comprendra des discussions avec le Centre de la sécurité des télécommunications Canada afin de préciser ou définir l'utilisation acceptable de la messagerie NIP à NIP.

Réponse d'Affaires indiennes et du Nord Canada : Affaires indiennes et du Nord Canada ne se conforme que partiellement aux lignes directrices du CSTC sur l'utilisation du BlackBerry et de la technologie NIP à NIP. La Division de la sécurité des TI, en collaboration avec d'autres intervenants de la GI/TI, termine actuellement une analyse de l'utilisation du BlackBerry au sein du Ministère. L'analyse évaluera la gestion et les contrôles techniques et opérationnels durant le cycle de vie des dispositifs BlackBerry, déterminera les risques et formulera des recommandations pour limiter le risque.

Les points d'accès sans fil offrent des degrés de protection variables

RECOMMANDATION

Santé Canada devrait passer en revue ses réseaux sans fil et s'assurer que les points d'accès sont dotés du cryptage de sécurité recommandé par le Centre de la sécurité des télécommunications Canada.

Réponse de Santé Canada : Santé Canada convient qu'un examen des réseaux sans fil devrait être effectué. Santé Canada s'emploiera à veiller à ce que tous les points d'accès sont dotés du cryptage de sécurité recommandé par le CSTC.

En général, les entités entreposent les dispositifs sans fil excédentaires de façon sécuritaire

RECOMMANDATION

Ressources humaines et Développement des compétences Canada devrait veiller à ce que tous ses dispositifs sans fil excédentaires soient entreposés dans des zones sécurisées.

Réponse de Ressources humaines et Développement des compétences Canada : Ressources humaines et Développement des compétences Canada accepte cette recommandation et mettra à jour sa directive d'orientation sur les dispositifs sans fil en conséquence.

Les données ne sont pas effacées de tous les téléphones intelligents et cellulaires

ECOMMANDATION

La Société canadienne d'hypothèques et de logement, le Service correctionnel du Canada, Santé Canada, et Ressources humaines et Développement des compétences Canada devraient établir des mécanismes de contrôle pour s'assurer que les données conservées dans les dispositifs sans fil excédentaires sont effacées avant la liquidation de ces dispositifs.

Réponse de la Société canadienne d'hypothèques et de logement : La SCHL suit un processus établi pour épurer les données qui se trouvent dans les téléphones excédentaires. Aucun problème n'a été signalé relativement au processus en place. La SCHL ajoutera un document dans chaque dossier pour indiquer ce qui a été fait.

Réponse du Service correctionnel du Canada : Le Service correctionnel du Canada est d'accord avec la recommandation et prépare actuellement un plan d'action pour remédier à la situation.

Réponse de Santé Canada : Santé Canada convient que des contrôles devraient être établis pour s'assurer que les données conservées dans les dispositifs sans fil excédentaires sont effacées avant le retrait des dispositifs. Santé Canada dispose actuellement de contrôles pour les nouveaux utilisateurs de téléphones cellulaires — un formulaire de consentement obligatoire — qui contient des renseignements détaillés, y compris une section regroupant les directives sur le retrait et le retour des téléphones cellulaires qui décrit le processus à suivre pour le retour des dispositifs.

Par ailleurs, Santé Canada modifie actuellement sa politique sur les dispositifs sans fil pour que cette dernière offre des directives détaillées à l'utilisateur d'un sans fil, à savoir les procédures et directives à suivre pour veiller à ce que les données conservées soient épurées/retirées avant le retrait des dispositifs.

Réponse de Ressources humaines et Développement des compétences Canada : Ressources humaines et Développement des Compétences Canada accepte cette recommandation. Le Ministère détruit physiquement ses dispositifs sans fil excédentaires et a déjà pris des mesures pour uniformiser le processus de destruction. En outre, le Ministères mettra à jour sa directive d'orientation sur les dispositifs sans fi pour faire en sorte que le processus amélioré sera communiqué à toutes les parties concernées.